



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/911,750      | 07/23/2001  | Charles M. Patton    | 10007237-1          | 4995             |

7590 02/22/2008  
HEWLETT-PACKARD COMPANY  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, CO 80527-2400

|          |
|----------|
| EXAMINER |
|----------|

DAVIS, ZACHARY A

|          |              |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2137

|           |               |
|-----------|---------------|
| MAIL DATE | DELIVERY MODE |
|-----------|---------------|

02/22/2008

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

|                              |                                      |                                      |  |
|------------------------------|--------------------------------------|--------------------------------------|--|
| <b>Office Action Summary</b> | <b>Application No.</b><br>09/911,750 | <b>Applicant(s)</b><br>PATTON ET AL. |  |
|                              | <b>Examiner</b><br>Zachary A. Davis  | <b>Art Unit</b><br>2137              |  |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 23 November 2007.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-12, 14, 15, 21-25, 27, 31-34, 36, 37, 42-44, 47-56 and 58-70 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-12, 14, 15, 21-25, 27, 31-34, 36, 37, 42-44, 47-56 and 58-70 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. A response was received on 23 November 2007. By this response, Claims 1, 15, 21, 27, 37, 44, 49-51, 54-56, 58, 60, 62, and 63 have been amended. Claims 26 and 57 have been canceled. New Claims 64-70 have been added. Claims 1-12, 14, 15, 21-25, 27, 31-34, 36, 37, 42-44, 47-56, and 58-70 are currently pending in the present application.

### ***Response to Arguments***

2. Applicant's arguments filed 23 November 2007 have been fully considered but they are not persuasive.

Claims 1-12, 14, 15, 62, and 63 were rejected under 35 U.S.C. 101 as directed to non-statutory subject matter. Claims 1-12, 14, 15, 21-27, 31-34, 37, 42-44, 47-57, and 59-63 were rejected under 35 U.S.C. 103(a) as unpatentable over Wiser et al, US Patent 6385596, in view of Fujiwara, US Patent Application Publication 2001/0054081, and Stefik et al, US Patent 6233684. Claims 36 and 58 were rejected under 35 U.S.C. 103(a) as unpatentable over Dwork et al, US Patent 6038316, in view of Fujiwara and Stefik.

Regarding the rejection under 35 U.S.C. 101, Applicant asserts that "The function performed by the computer processing the data structure stored on the medium using the key is to reveal in clear form the digital string having value to the purchaser that has

been embedded in the preexisting digital file in a hidden manner” and that this “constitutes a useful, concrete, and tangible result **when used in a computer system**” (see page 15 of the present response, emphasis added). Applicant further asserts that “The data manipulation that the file supports is the extraction, using the key, of the hidden digital string from the file in clear form” (page 15 of the present response). The Examiner respectfully disagrees. Although Claim 1, for example, recites that “said embedded digital file on said processor readable medium is **processable by a computer program**” (emphasis added), the Examiner notes that this only recites a capability of the embedded digital file. Although the file is “processable” (i.e. able to be processed by something else, namely the recited computer program), the file does not provide any functionality for the processing itself (i.e. the embedded file does not provide any instructions, for example, that would cause such a computer program to perform the processing). The Examiner further notes that the assertion that the claim produces “a useful, concrete and tangible result when used in a computer system” suggests that what is actually claimed (the digital file and encrypted and embedded string in the file, on a processor readable medium) is not necessarily used in a computer system, and without that use, there is no function that the alleged “data structure” clearly supports. Once again, the Examiner notes that Claims 1 and 15, for example, are directed to the arrangement of the pieces of data that would result from a method such as that recited in Claim 21, rather than providing the functionality of the method themselves. The claims also do not provide functionality for actually using those resulting pieces of data to perform further actions or processing, but merely recite the

pieces of data themselves. There is no function that the arranged pieces of data perform themselves.

Regarding the rejections under 35 U.S.C. 103(a), and specifically with reference to independent Claim 1, Applicant argues that the digital work of Stefik does not include any watermark and thus does not include the digital string, and that the watermark is only applied when the document is printed (page 20 of the present response). The Examiner respectfully disagrees. First, the Examiner notes that Stefik discloses many other rendering options aside from printing and therefore the watermark is not only present during printing (Stefik, column 7, lines 11-20, for example). Further, in response to applicant's argument that Stefik does not disclose using the key to reveal the digital string and that the encrypted document does not contain an encrypted string (page 20 of the present response), the Examiner notes that the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). In particular, the Examiner notes that Stefik was not the only reference relied upon for a teaching that the string can be revealed using a key, noting that Wiser also discloses that the string is encrypted (column 9, lines 19-20) and Fujiwara discloses the string embedded in the file (paragraphs 0047, 0049, and 0054).

Also regarding Claim 1, in response to applicant's arguments against the references individually (see pages 20-21 of the present response), one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Specifically, Applicant argues that Stefik does not use the key to modify the digital string. First, the Examiner disagrees, noting that Stefik generally discloses that the key is made publicly available, as claimed, and a file can be processed using the key to reveal the string in clear form (see column 16, line 51-column 18, line 5, as previously cited, generally regarding the use of a public key; see also column 13, lines 48-67, where the embedded data is extracted and read out in human readable form). Further, the Examiner notes that Wiser also discloses that the digital string is encrypted ("modified with a key", as claimed; see column 9, lines 19-20, as previously cited). Therefore, the combination at least discloses the claimed limitations.

Also regarding Claim 1, Applicant alleges that the reasoning stated in the previous Office actions to combine Wiser and Fujiwara does not have a sufficient rational underpinning, because, as Applicant asserts, they have the same purpose (pages 21-22 of the present response). In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally

available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the motivation was as cited in the previous Office actions, namely to effectively prevent illegal copying (see Fujiwara, page 5, paragraph 0049). Further motivation may be found in Fujiwara, namely to allow a system to respond to diverse demands of users and securely distribute content (Fujiwara, page 1, paragraph 0010). Additionally, the Examiner clarifies that further suggestion to combine the references would be found in the fact that, given that both Wiser and Fujiwara disclose including personal data in some form with delivered content in order to discourage illegal copying of that data (see Fujiwara, paragraph 0049, and Wiser, column 8, lines 53-56), but provide different specifics in those methods (i.e. Fujiwara embeds the personal data directly in the content file, while Wiser embeds the personal data in a passport linked to the content file), it would have been obvious to one of ordinary skill in the art to try the alternate location for embedding the personal data because it would have yielded the predictable result of providing the same function through a different implementation.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning (pages 22 and 23 of the present response), it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the

applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Additionally in reference to Claim 1, Applicant asserts that the motivation to combine Stefik and Wiser also does not have sufficient rational underpinning to serve as a valid reason to combine, because the Wiser reference does not disclose any visible strings of the purchaser's personal information (see pages 22-23 of the present response). First, the Examiner notes that Applicant has apparently ignored the use of the Fujiwara reference in making this argument, noting that Fujiwara clearly does disclose the use of a visible string embedded in the file (see paragraph 0049). Further, the Examiner notes that Wiser also discloses visible personal information (see abstract, where confidential information of the purchaser is displayed).

Regarding independent Claims 37 and 62, Applicant refers back to the arguments in reference to Claim 1 (see pages 23-24 of the present response). In response, the Examiner notes that the above responses referring to Claim 1 are applicable as appropriate to Claims 37 and 62.

In reference to independent Claim 21, Applicant argues that none of the cited references disclose embedding a provider string announcing a reward for detecting that the file was illicitly distributed to a party other than the purchaser (page 25 of the present response). Although Applicant alleges that this limitation was previously recited in dependent Claim 26, the Examiner notes that the limitation recited in now-canceled Claim 26 was not of the same scope as the limitation recited in amended Claim 21; in particular, Claim 26 used the indefinite term "inappropriately distributed", whereas the

amended Claim 21 uses the term “illicitly distributed”. While this is also potentially dependent on a changing standard, the plain meaning of the terms does not appear to render the claim language indefinite. Regarding the substantive argument as to whether the cited art teaches the newly amended limitation, the Examiner notes that new grounds of rejection have been set forth below, rendering Applicant’s argument on this point moot. It is noted that this new ground of rejection is considered to be necessitated by amendment because the scope has changed from dependent Claim 26 as noted above.

Regarding the argument with respect to Claim 21 that there is no suggestion or motivation to combine the references (page 25 of the present response), the Examiner has responded to similar arguments as applied in reference to Claim 1 above.

Regarding independent Claims 15 and 44, Applicant refers back to the arguments in reference to Claim 21 (see pages 26-27 of the present response). In response, the Examiner notes that the above responses referring to Claim 21 are applicable as appropriate to Claims 15 and 44.

Regarding dependent Claim 3, Applicant argues that the cited prior art does not teach or suggest an encrypted private digital string and an encrypted public digital string (see pages 27-28 of the present response). However, the Examiner first notes that as cited, the prior art does disclose encryption with both public and private keys (see, for example, Wiser, column 9, lines 19-20, where a private key is explicitly disclosed, and column 4, lines 13-41, explicitly disclosing the use of public keys; see also Stefik, column 16, line 51-column 18, line 5, as previously cited). Further, the Examiner notes

that there does not appear to be a clear enabling disclosure in the present specification of the use of a private digital string and a public digital string. **Applicant is respectfully requested to point out in the specification where enabling disclosure under 35 U.S.C. 112, first paragraph, is provided for the limitations of Claim 3.**

Regarding dependent Claims 51, 53, and 55, Applicant argues that the cited art does not disclose various features recited therein (pages 28-30 of the present response). In response, the Examiner notes that because those claims were subject to a rejection under 35 U.S.C. 112, second paragraph, as indefinite, it had not been possible to fully determine the scope of those claims, and therefore the claims were rejected to the extent possible. As the rejection under 35 U.S.C. 112, second paragraph, has been overcome except as noted below, the Examiner sets forth below more detailed reasoning as to the grounds of rejection under 35 U.S.C. 103(a).

Regarding Claim 36, in response to applicant's argument that the digital string is not stored in the document key of the Stefik reference and therefore no disclosure that the digital string can be recovered from a key (page 32 of the present response), the Examiner notes that the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). In particular, the Examiner notes that Stefik was not the only reference relied upon for a teaching that the string can be revealed using a key, noting

that Dwork also discloses that the string is encrypted (column 7, lines 14-19) and Fujiwara discloses the string embedded in the file (paragraphs 0047, 0049, and 0054).

Further regarding Claim 36, Applicant asserts that there is not sufficient rational underpinning to serve as a reason to combine the references, similar to the arguments presented with respect to Claim 1 (see pages 32-34 of the present response). The Examiner notes that similar motivation and clarification can be applied to Claim 36, and directs Applicant to the responses above in reference to Claim 1, *mutatis mutandis*.

Applicant additionally asserts that the combination of Dwork and Fujiwara would render Dwork inoperative, because mass distribution of content files would not be possible if each individual copy of the files had to be customized as taught by Fujiwara (pages 33-34 of the present response). However, Applicant has not provided any evidence in support of the assertion that mass distribution would not be possible, which renders the assertion a mere allegation. If anything, it appears that it would only add additional overhead to the process, but would not render it impossible as alleged.

Regarding new Claims 65, 67, 69, and 70, Applicant argues that none of the cited art discloses anything besides using public key encryption, which requires an additional key (namely, the corresponding private key) and does not meet the new limitation that no additional key is used to reveal the embedded string in clear form (see pages 35-36 of the present response). However, first, the Examiner notes that the only keys disclosed in the present specification appear to keys of public/private key pairs. Further, the Examiner notes that the cited prior art does, in fact, disclose other keys

aside from asymmetric key pairs, in contrast to the present application (see Wisner, column 21, lines 45-52; Stefik, column 14, lines 62-67, for example).

Regarding new Claims 66 and 68, although Applicant asserts that the cited references do not disclose the newly claimed limitations (page 36 of the present response), the Examiner notes that the new limitations appear to render the claims indefinite because they contradict the independent claims as detailed below.

Therefore, for the reasons detailed above, the Examiner maintains the rejections as set forth below.

### ***Specification***

3. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: The specification does not provide proper antecedent basis for the subject matter of Claim 58 as amended or for new Claims 65, 67, 69, or 70. In particular, there is not sufficient antecedent basis for the limitations regarding the use of “no additional key” or similar in those claims. Additionally, there is insufficient antecedent basis in the specification for the limitation in Claim 55 that another key is made available “at a second time later than the first time”. For further detail, see below regarding the rejection under 35 U.S.C. 112, first paragraph, for failure to comply with the written description requirement.

***Claim Rejections - 35 USC § 101***

4. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 1-12, 14, 15, 62, 63, 65, 66, and 69 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1-12, 14, 15, 62, 63, 65, 66, and 69 are directed merely to arrangements of data, although stored in a processor readable medium. Specifically, the independent claims recite a digital file and at least one digital string arranged as embedded within the file. An arrangement of data is non-functional descriptive material, which is not statutory subject matter even if stored in a computer-readable medium. See MPEP § 2106.01.

***Claim Rejections - 35 USC § 112***

6. The rejection of Claims 1-12, 14, 26, 27, 37, 47-51, 53, 55-57, 60, and 63 as rejected under 35 U.S.C. 112, second paragraph, as indefinite is withdrawn in light of the amendments to the claims or moot in light of the cancellation of the claims, as applicable. However, some of the issues of indefiniteness noted in the previous Office action have not been addressed, and the amendments to the claims have raised new issues of indefiniteness, and therefore, the rejection of Claims 52, 54, and 58 is NOT withdrawn, and new Claims 65-70 are additionally rejected under 35 U.S.C. 112, second paragraph, as set forth below.

7. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

8. Claims 55, 58, and 65, 67, 69, and 70 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim 55 recites the limitation that “another one of the encryption keys is made publicly available by said provider at a second time later than the first time”. There is not sufficient written description of this limitation in the present specification. In particular, there is no mention of a time at which keys are provided, or of a time at which a key is made available is later than a time at which a prior key was made available. It is noted that because the claim was previously rendered indefinite, it was not possible to fully make a determination of sufficiency of written description; because the amendment to the claim has corrected the issues of indefiniteness, it has become clear that there is not sufficient written description for the claimed limitation, and therefore this rejection was necessitated by the amendment.

Claim 58 recites the limitation that a program recovers the string in clear form from the decryption key “without using said any additional key”. Similarly, Claims 65, 67, and 69 recite revealing or extracting a string “using said key but no additional key”,

and Claim 70 recites recovering a string “without using any additional key”. There does not appear to be any description of such a negative limitation in the specification. It is noted that the absence of a positive recitation is not basis for an exclusion. See MPEP § 2173.05(i). It is also noted that Applicant appears to equate this limitation to using other than public key (i.e. asymmetric) encryption in the present arguments (see pages 35-36 of the present response); however, it is noted that the only keys that are described in the specification are asymmetric (i.e. public/private) key pairs, and therefore, there does not appear to be a suggestion of using any different form of key.

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 52, 54, 58, and 65-70 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 52 recites the limitation “all of the encryption keys”; there does not appear to be sufficient antecedent basis for this limitation in the claims.

Claim 54 recites the limitation “the purchase of said valued content”. There is insufficient antecedent basis for this limitation in the claims.

Claim 58 recites the limitation of recovering the string in clear form “without using said any additional key”. First, there is insufficient antecedent basis for the limitation “said any additional key” in the claims. Further, the negative limitation as a whole is generally unclear. Specifically,

Claims 65, 67, and 69 recite the limitation of “using said key but no additional key” to reveal or extract a string, and Claim 70 similarly recites recovering a string “without using any additional key”. The negative limitations are generally unclear. In particular,

Claim 66 recites “said embedded digital file on said processor readable medium is not processable by said computer program using said key to reveal said preexisting digital file in clear form”. This limitation appears to contradict the limitations of independent Claim 1, from which Claim 66 depends, because there is no suggestion in Claim 1 that the preexisting digital file is in anything but clear form, and therefore it is immaterial as to whether a key can reveal it in clear form.

Similarly, Claim 68 recites “said preexisting digital file is not extractable in clear form from said second digital file using said key”; however, there is nothing in independent Claim 37, from which Claim 68 depends, to suggest that the file is in anything but clear form.

11. The Examiner notes that, due to the issues of indefiniteness regarding new Claims 65-70 and insufficient written description regarding new Claims 65, 67, 69, and 70, it has not been possible to construe the claims to the extent necessary to determine the scope of those claims such that a determination of patentability with respect to novelty under 35 U.S.C. 102 or non-obviousness under 35 U.S.C. 103 could be made.

***Claim Rejections - 35 USC § 103***

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

13. Claims 1-12, 14, 37, 42, 43, 47, 48, and 62-64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiser et al, US Patent 6385596, in view of Fujiwara, US Patent Application Publication 2001/0054081, and Stefik et al, US Patent 6233684.

In reference to Claim 1, Wiser discloses valued content in a computer readable-medium including a digital file having independent value to a provider (column 6, lines 48-52) and a digital string having a latent value to a purchaser embedded in a passport that is linked to the digital file (column 8, lines 53-56, where the string is personal information). Wiser further discloses that the string is provided in clear form and modified according to a key (column 9, lines 19-20). However, although Wiser discloses that the string is embedded in the passport linked to the file (column 6, lines 44-46), Wiser does not explicitly disclose also embedding the personal information in the file itself.

Fujiwara discloses a system for content delivery in which personal data is embedded in a delivered digital file (page 4, paragraph 0047; page 5, paragraphs 0049 and 0054). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made modify the content of Wiser to include the string also

embedded directly in the digital file, in order to effectively prevent illegal copying (see Fujiwara, page 5, paragraph 0049) and to allow a system to respond to diverse demands of users and securely distribute content (Fujiwara, page 1, paragraph 0010). Additionally, given that both Wiser and Fujiwara disclose including personal data in some form with delivered content in order to discourage illegal copying of that data (see Fujiwara, paragraph 0049, and Wiser, column 8, lines 53-56), but provide different specifics in those methods (i.e. Fujiwara embeds the personal data directly in the content file, while Wiser embeds the personal data in a passport linked to the content file), it would have been obvious to one of ordinary skill in the art to try the alternate location for embedding the personal data because it would have yielded the predictable result of providing the same function through a different implementation.

Although Wiser and Fujiwara disclose watermarks (Wiser, column 7, lines 5-6 and 17-26) and a string embedded in a digital file (Fujiwara, page 4, paragraph 0047; page 5, paragraphs 0049 and 0054), neither Wiser nor Fujiwara explicitly discloses embedding the string multiple times nor in a hidden manner. Stefik discloses a system for controlling use of digital works in which multiple watermarks may be embedded within a digital work, and both visible and invisible (i.e. hidden) watermarks may be used (column 8, lines 51-55). Stefik further discloses that the provider makes the key publicly available and that the file can be processed using the key to reveal the string in clear form (column 16, line 51-column 18, line 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the content of Wiser and Fujiwara to include the string embedded two or more times, at least once

in a hidden manner, in order to increase robustness; that is, even if the visible string(s) is/are somehow removed, the invisible one(s) would remain and still allow control of the digital rights (see Stefik, column 8, lines 55-56).

In reference to Claims 2, 3, 47, and 48, Wiser, Fujiwara, and Stefik further disclose that the string is encrypted, using a private or public key (Wiser, column 9, lines 19-20; Stefik, column 16, line 51-column 18, line 5).

In reference to Claim 4, Wiser, Fujiwara, and Stefik further disclose the string being embedded in a human perceptible form (Wiser, column 9, lines 16-18; Fujiwara, page 5, paragraph 0049; Stefik, column 8, lines 51-55).

In reference to Claim 5, Wiser, Fujiwara, and Stefik further disclose a digital watermark (Wiser, column 7, lines 5-6 and 17-26; Stefik, column 8, lines 51-55).

In reference to Claims 6-9, Wiser, Fujiwara, and Stefik further disclose that the file can include text, images, video, and audio (Wiser, column 6, lines 59-60, for text and images; Wiser, column 6, lines 48-52; column 7, lines 4-9 for audio; Fujiwara, for example, page 6, paragraph 0057 for text, images, and audio; Stefik, column 5, lines 35-40, for text, images, audio, and video).

In reference to Claim 10, Wiser, Fujiwara, and Stefik further disclose that the latent value of the string resides in information that would place the purchaser at increased financial risk if known by another (Wiser, column 8, lines 53-56).

In reference to Claims 11 and 12, Wiser, Fujiwara, and Stefik further disclose a provider string that can be encrypted (see Wiser, column 4, lines 1-4; column 7, lines 27-46; see also column 10, line 60-column 11, line 7).

In reference to Claim 14, Wiser, Fujiwara, and Stefik further disclose recording the file on a portable medium (see Wiser, column 9, line 53-column 10, line 16).

In reference to Claim 37, Wiser discloses a system including a processor (see, for example, Figure 1, Client System 126; see also column 9, lines 40-52), a storage device (for example, see column 10, lines 50-55), an interface, and content including a digital file (column 6, lines 48-52) and a string embedded in a passport that is linked to the digital file (column 8, lines 53-56). Wiser further discloses that the string is provided in clear form and modified according to a key (column 9, lines 19-20). However, although Wiser discloses that the string is embedded in the passport linked to the file (column 6, lines 44-46), Wiser does not explicitly disclose also embedding the personal information in the file itself.

Fujiwara discloses a system for content delivery in which personal data is embedded in a delivered digital file (page 4, paragraph 0047; page 5, paragraphs 0049 and 0054). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made modify the system of Wiser to include the string also embedded directly in the digital file, in order to effectively prevent illegal copying (see Fujiwara, page 5, paragraph 0049) and to allow a system to respond to diverse demands of users and securely distribute content (Fujiwara, page 1, paragraph 0010). Additionally, given that both Wiser and Fujiwara disclose including personal data in some form with delivered content in order to discourage illegal copying of that data (see Fujiwara, paragraph 0049, and Wiser, column 8, lines 53-56), but provide different

specifics in those methods (i.e. Fujiwara embeds the personal data directly in the content file, while Wiser embeds the personal data in a passport linked to the content file), it would have been obvious to one of ordinary skill in the art to try the alternate location for embedding the personal data because it would have yielded the predictable result of providing the same function through a different implementation.

Although Wiser and Fujiwara disclose watermarks (Wiser, column 7, lines 5-6 and 17-26) and a string embedded in a digital file (Fujiwara, page 4, paragraph 0047; page 5, paragraphs 0049 and 0054), neither Wiser nor Fujiwara explicitly discloses embedding the string multiple times nor in a hidden manner. Stefik discloses a system for controlling use of digital works in which multiple watermarks may be embedded within a digital work, and both visible and invisible (i.e. hidden) watermarks may be used (column 8, lines 51-55). Stefik further discloses that the provider makes the key publicly available and that the file can be processed using the key to reveal the string in clear form (column 16, line 51-column 18, line 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the content of Wiser and Fujiwara to include the string embedded two or more times, at least once in a hidden manner, in order to increase robustness; that is, even if the visible string(s) is/are somehow removed, the invisible one(s) would remain and still allow control of the digital rights (see Stefik, column 8, lines 55-56).

In reference to Claims 42 and 43, Wiser, Fujiwara, and Stefik further disclose a point of sale machine and a network connection (Wiser, see column 11, lines 8-13).

In reference to Claim 62, Wiser discloses valued content in a computer readable-medium including a digital file having independent value to a provider (column 6, lines 48-52) and a digital string having a latent value to a purchaser embedded in a passport that is linked to the digital file (column 8, lines 53-56, where the string is personal information). Wiser further discloses that the string is provided in clear form and modified according to a key (column 9, lines 19-20). However, although Wiser discloses that the string is embedded in the passport linked to the file (column 6, lines 44-46), Wiser does not explicitly disclose also embedding the personal information in the file itself.

Fujiwara discloses a system for content delivery in which personal data is embedded in a delivered digital file (page 4, paragraph 0047; page 5, paragraphs 0049 and 0054). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made modify the content of Wiser to include the string also embedded directly in the digital file, in order to effectively prevent illegal copying (see Fujiwara, page 5, paragraph 0049) and to allow a system to respond to diverse demands of users and securely distribute content (Fujiwara, page 1, paragraph 0010). Additionally, given that both Wiser and Fujiwara disclose including personal data in some form with delivered content in order to discourage illegal copying of that data (see Fujiwara, paragraph 0049, and Wiser, column 8, lines 53-56), but provide different specifics in those methods (i.e. Fujiwara embeds the personal data directly in the content file, while Wiser embeds the personal data in a passport linked to the content file), it would have been obvious to one of ordinary skill in the art to try the alternate

location for embedding the personal data because it would have yielded the predictable result of providing the same function through a different implementation.

Although Wiser and Fujiwara disclose watermarks (Wiser, column 7, lines 5-6 and 17-26) and a string embedded in a digital file (Fujiwara, page 4, paragraph 0047; page 5, paragraphs 0049 and 0054), neither Wiser nor Fujiwara explicitly discloses embedding the string multiple times nor in a hidden manner. Stefik discloses a system for controlling use of digital works in which multiple watermarks may be embedded within a digital work, and both visible and invisible (i.e. hidden) watermarks may be used (column 8, lines 51-55). Stefik further discloses that the provider makes the key publicly available and that the file can be processed using the key to reveal the string in clear form (column 16, line 51-column 18, line 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the content of Wiser and Fujiwara to include the string embedded two or more times, at least once in a hidden manner, in order to increase robustness; that is, even if the visible string(s) is/are somehow removed, the invisible one(s) would remain and still allow control of the digital rights (see Stefik, column 8, lines 55-56).

In reference to Claim 63, Wiser, Fujiwara, and Stefik further disclose two different strings formed using different encryption keys (see Stefik, column 8, lines 51-55 and column 16, line 51-column 18, line 5).

In reference to Claim 64, Wiser discloses a method including acquiring a digital string, modifying the digital string (column 9, lines 19-20), embedding the string in a

passport that is linked to the digital file (column 8, lines 53-56), embedding a provider string (see column 4, lines 1-4; column 7, lines 27-46), and conveying the file to a purchaser (column 9, lines 54-56). However, although Wiser discloses that the string is embedded in the passport linked to the file (column 6, lines 44-46), Wiser does not explicitly disclose also embedding the personal information in the file itself.

Fujiwara discloses a method for content delivery in which personal data is embedded in a delivered digital file (page 4, paragraph 0047; page 5, paragraphs 0049 and 0054). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made modify the method of Wiser to include embedding the string directly in the digital file, in order to effectively prevent illegal copying (see Fujiwara, page 5, paragraph 0049) and to allow a system to respond to diverse demands of users and securely distribute content (Fujiwara, page 1, paragraph 0010). Additionally, given that both Wiser and Fujiwara disclose including personal data in some form with delivered content in order to discourage illegal copying of that data (see Fujiwara, paragraph 0049, and Wiser, column 8, lines 53-56), but provide different specifics in those methods (i.e. Fujiwara embeds the personal data directly in the content file, while Wiser embeds the personal data in a passport linked to the content file), it would have been obvious to one of ordinary skill in the art to try the alternate location for embedding the personal data because it would have yielded the predictable result of providing the same function through a different implementation.

Although Wiser and Fujiwara disclose watermarks (Wiser, column 7, lines 5-6 and 17-26) and a string embedded in a digital file (Fujiwara, page 4, paragraph 0047;

page 5, paragraphs 0049 and 0054), neither Wiser nor Fujiwara explicitly discloses embedding the string multiple times nor in a hidden manner. Stefik discloses a method for controlling use of digital works in which multiple watermarks may be embedded within a digital work, and both visible and invisible (i.e. hidden) watermarks may be used, where the multiple watermarking methods form different modified strings (column 8, lines 51-55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the content of Wiser and Fujiwara to include the string embedded two or more times, at least once in a hidden manner, in order to increase robustness; that is, even if the visible string(s) is/are somehow removed, the invisible one(s) would remain and still allow control of the digital rights (see Stefik, column 8, lines 55-56).

14. Claims 15, 21-25, 27, 31-34, 44, 49-56, and 59-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiser, in view of Fujiwara, Stefik, and DeTreville, US Patent Application Publication 2002/0156743.

In reference to Claim 15, Wiser discloses valued content in a computer readable-medium including a digital file having independent value to a provider (column 6, lines 48-52), a digital string having a latent value to a purchaser embedded in a passport that is linked to the digital file (column 8, lines 53-56) and is encrypted (column 9, lines 19-20), and an encrypted provider digital string (see column 4, lines 1-4; column 7, lines 27-46). However, although Wiser discloses that the string is embedded in the passport

linked to the file (column 6, lines 44-46), Wiser does not explicitly disclose also embedding the personal information in the file itself.

Fujiwara discloses a system for content delivery in which personal data is embedded in a delivered digital file (page 4, paragraph 0047; page 5, paragraphs 0049 and 0054). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made modify the content of Wiser to include the string also embedded directly in the digital file, in order to effectively prevent illegal copying (see Fujiwara, page 5, paragraph 0049) and to allow a system to respond to diverse demands of users and securely distribute content (Fujiwara, page 1, paragraph 0010). Additionally, given that both Wiser and Fujiwara disclose including personal data in some form with delivered content in order to discourage illegal copying of that data (see Fujiwara, paragraph 0049, and Wiser, column 8, lines 53-56), but provide different specifics in those methods (i.e. Fujiwara embeds the personal data directly in the content file, while Wiser embeds the personal data in a passport linked to the content file), it would have been obvious to one of ordinary skill in the art to try the alternate location for embedding the personal data because it would have yielded the predictable result of providing the same function through a different implementation.

Although Wiser and Fujiwara disclose watermarks (Wiser, column 7, lines 5-6 and 17-26) and a string embedded in a digital file (Fujiwara, page 4, paragraph 0047; page 5, paragraphs 0049 and 0054), neither Wiser nor Fujiwara explicitly discloses embedding the string multiple times. Stefik discloses a system for controlling use of digital works in which multiple watermarks may be embedded within a digital work

(column 8, lines 51-55). Stefik also discloses an encrypted provider string (column 3, lines 31-35). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the content of Wiser and Fujiwara to include the string embedded two or more times, at least once in a hidden manner, in order to increase robustness; that is, even if the visible string(s) is/are somehow removed, the invisible one(s) would remain and still allow control of the digital rights (see Stefik, column 8, lines 55-56).

Although Wiser, Fujiwara, and Stefik disclose the inclusion of a provider digital string (see Wiser, column 4, lines 1-4; column 7, lines 27-46; Stefik, column 3, lines 51-55), none of Wiser, Fujiwara, and Stefik explicitly discloses that the provider digital string includes a notice of a reward for detecting illicit distribution of the valued content. DeTreville discloses a system for detecting pirated content that includes providing to a user notification of a reward for detecting that valued content has been distributed illicitly to other than the purchaser (page 5, paragraph 0040). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the content of Wiser, Fujiwara, and Stefik to include the provider string with a notice of a reward, in order to provide incentive to a user to assist in identifying the source of unauthorized copies (see DeTreville, paragraph 0040).

In reference to Claim 21, Wiser discloses a method including acquiring a digital string, modifying the digital string (column 9, lines 19-20), embedding the string in a passport that is linked to the digital file (column 8, lines 53-56), embedding a provider

string (see column 4, lines 1-4; column 7, lines 27-46), and conveying the file to a purchaser (column 9, lines 54-56). However, although Wiser discloses that the string is embedded in the passport linked to the file (column 6, lines 44-46), Wiser does not explicitly disclose also embedding the personal information in the file itself.

Fujiwara discloses a method for content delivery in which personal data is embedded in a delivered digital file (page 4, paragraph 0047; page 5, paragraphs 0049 and 0054). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made modify the method of Wiser to include embedding the string directly in the digital file, in order to effectively prevent illegal copying (see Fujiwara, page 5, paragraph 0049) and to allow a system to respond to diverse demands of users and securely distribute content (Fujiwara, page 1, paragraph 0010). Additionally, given that both Wiser and Fujiwara disclose including personal data in some form with delivered content in order to discourage illegal copying of that data (see Fujiwara, paragraph 0049, and Wiser, column 8, lines 53-56), but provide different specifics in those methods (i.e. Fujiwara embeds the personal data directly in the content file, while Wiser embeds the personal data in a passport linked to the content file), it would have been obvious to one of ordinary skill in the art to try the alternate location for embedding the personal data because it would have yielded the predictable result of providing the same function through a different implementation.

Although Wiser and Fujiwara disclose watermarks (Wiser, column 7, lines 5-6 and 17-26) and a string embedded in a digital file (Fujiwara, page 4, paragraph 0047; page 5, paragraphs 0049 and 0054), neither Wiser nor Fujiwara explicitly discloses

embedding the string multiple times nor in a hidden manner. Stefik discloses a method for controlling use of digital works in which multiple watermarks may be embedded within a digital work, and both visible and invisible (i.e. hidden) watermarks may be used, where the multiple watermarking methods form different modified strings (column 8, lines 51-55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the content of Wiser and Fujiwara to include the string embedded two or more times, at least once in a hidden manner, in order to increase robustness; that is, even if the visible string(s) is/are somehow removed, the invisible one(s) would remain and still allow control of the digital rights (see Stefik, column 8, lines 55-56).

Although Wiser, Fujiwara, and Stefik disclose the embedding of a provider digital string (see Wiser, column 4, lines 1-4; column 7, lines 27-46; Stefik, column 3, lines 51-55), none of Wiser, Fujiwara, and Stefik explicitly discloses that the provider digital string includes a notice of a reward for detecting illicit distribution of the valued content. DeTreville discloses a system for detecting pirated content that includes providing to a user notification of a reward for detecting that valued content has been distributed illicitly to other than the purchaser (page 5, paragraph 0040). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Wiser, Fujiwara, and Stefik to include the provider string with a notice of a reward, in order to provide incentive to a user to assist in identifying the source of unauthorized copies (see DeTreville, paragraph 0040).

In reference to Claims 22-24, Wiser, Fujiwara, Stefik, and DeTreville further disclose encrypting the digital string using public or private keys (Wiser, column 9, lines 19-20; Stefik, column 16, line 51-column 18, line 5).

In reference to Claim 25, Wiser, Fujiwara, Stefik, and DeTreville further disclose generating a digital watermark (Wiser, column 7, lines 5-6 and 17-26; Stefik, column 10, lines 20-22; column 8, lines 51-55).

In reference to Claims 27, Wiser, Fujiwara, Stefik, and DeTreville further disclose that the provider string can be encrypted (see Wiser, column 4, lines 1-4; column 7, lines 27-46; see also column 10, line 60-column 11, line 7; Stefik column 3, lines 51-55).

In reference to Claims 31-33, Wiser, Fujiwara, Stefik, and DeTreville further discloses that the string can be embedded in images, audio, or video (Wiser, column 6, lines 59-60, for images; Wiser, column 6, lines 48-52; column 7, lines 4-9 for audio; Fujiwara, for example, page 6, paragraph 0057 for images, and audio; Stefik, column 5, lines 35-40, for images, audio, and video).

In reference to Claim 34, Wiser, Fujiwara, Stefik, and DeTreville further disclose that the latent value of the string resides in information that would place the purchaser at increased financial risk if known by another (Wiser, column 8, lines 53-56).

In reference to Claims 49, 50, 52, and 55, Wiser, Fujiwara, Stefik, and DeTreville further disclose that at least one key is made publicly available by the provider (Stefik, column 16, line 51-column 18, line 5; see in particular column 16, line 64-column 17, line 3, where there is a document key for each document).

In reference to Claims 51 and 56, Wiser, Fujiwara, Stefik, and DeTreville further disclose a process or computer program to extract or reveal the string is made publicly available by the provider (Stefik, column 16, line 51-column 18, line 5, where the public key encryption/decryption algorithm is inherently made available, otherwise, the public key would be useless).

In reference to Claims 53 and 54, Wiser, Fujiwara, Stefik, and DeTreville further disclose informing the purchaser that at least one key has been made publicly available (Stefik, column 16, line 51-column 18, line 5, where the key is made available; column 15, line 66-column 16, line 5, where the user must be aware that the key is publicly available; see also column 10, lines 1-5; see also DeTreville, paragraph 0041).

In reference to Claim 44, Wiser discloses a system including a processor (column 9, lines 40-52), an interface that requests a digital string (column 8, lines 53-56), and a storage device (for example, column 10, lines 50-55). Wiser further discloses embedding the string in a passport that is linked to a digital file (column 8, lines 53-56). Wiser further discloses that the string is provided in clear form and modified according to a key (column 9, lines 19-20). However, although Wiser discloses that the string is embedded in the passport linked to the file (column 6, lines 44-46), Wiser does not explicitly disclose also embedding the personal information in the file itself.

Fujiwara discloses a system for content delivery in which personal data is embedded in a delivered digital file (page 4, paragraph 0047; page 5, paragraphs 0049

and 0054). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made modify the system of Wiser to embed the string directly in the digital file, in order to effectively prevent illegal copying (see Fujiwara, page 5, paragraph 0049) and to allow a system to respond to diverse demands of users and securely distribute content (Fujiwara, page 1, paragraph 0010). Additionally, given that both Wiser and Fujiwara disclose including personal data in some form with delivered content in order to discourage illegal copying of that data (see Fujiwara, paragraph 0049, and Wiser, column 8, lines 53-56), but provide different specifics in those methods (i.e. Fujiwara embeds the personal data directly in the content file, while Wiser embeds the personal data in a passport linked to the content file), it would have been obvious to one of ordinary skill in the art to try the alternate location for embedding the personal data because it would have yielded the predictable result of providing the same function through a different implementation.

Although Wiser and Fujiwara disclose watermarks (Wiser, column 7, lines 5-6 and 17-26) and a string embedded in a digital file (Fujiwara, page 4, paragraph 0047; page 5, paragraphs 0049 and 0054), neither Wiser nor Fujiwara explicitly discloses embedding the string multiple times nor in a hidden manner. Stefik discloses a method for controlling use of digital works in which multiple watermarks may be embedded within a digital work, and both visible and invisible (i.e. hidden) watermarks may be used, where the multiple watermarking methods form different modified strings (column 8, lines 51-55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the content of Wiser and Fujiwara to

include the string embedded two or more times, at least once in a hidden manner, in order to increase robustness; that is, even if the visible string(s) is/are somehow removed, the invisible one(s) would remain and still allow control of the digital rights (see Stefik, column 8, lines 55-56).

Although Wiser, Fujiwara, and Stefik disclose the string embedded in a digital file (Fujiwara, page 4, paragraph 0047; page 5, paragraphs 0049 and 0054), none of Wiser, Fujiwara, and Stefik explicitly discloses that the purchaser digital string includes a notice of a reward for detecting illicit distribution of the valued content. DeTreville discloses a system for detecting pirated content that includes providing to a user notification of a reward for detecting that valued content has been distributed illicitly to other than the purchaser (page 5, paragraph 0040). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Wiser, Fujiwara, and Stefik to include the purchaser string with a notice of a reward, in order to provide incentive to a user to assist in identifying the source of unauthorized copies (see DeTreville, paragraph 0040).

In reference to Claims 59 and 60, Wiser, Fujiwara, Stefik, and DeTreville further disclose two different strings formed using different encryption keys (see Stefik, column 8, lines 51-55 and column 16, line 51-column 18, line 5).

In reference to Claim 61, Wiser, Fujiwara, Stefik, and DeTreville further disclose embedding at least one modified string a plurality of times (Stefik, column 8, lines 51-55).

15. Claims 36 and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dwork et al, US Patent 6038316, in view of Fujiwara and Stefik.

In reference to Claim 36, Dwork discloses acquiring a digital string (column 7, lines 40-47), encrypting a digital string and embedding the string in a decryption key (column 7, lines 14-19), encrypting a digital file (column 7, lines 34-37), and conveying the encrypted file to a purchaser (column 7, lines 38-40). However, Dwork does not explicitly disclose also embedding the digital string in the digital file that is encrypted.

Fujiwara discloses a method for content delivery in which personal data is embedded in a delivered digital file (page 4, paragraph 0047; page 5, paragraphs 0049 and 0054). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made modify the method of Dwork to include embedding the string directly in the digital file before encryption, in order to effectively prevent illegal copying (see Fujiwara, page 5, paragraph 0049) and to allow a system to respond to diverse demands of users and securely distribute content (Fujiwara, page 1, paragraph 0010). Additionally, given that both Dwork and Fujiwara disclose including personal data in some form with delivered content in order to discourage illegal copying of that data (see Fujiwara, paragraph 0049, and Dwork, column 12, lines 21-34), but provide different specifics in those methods (i.e. Fujiwara embeds the personal data directly in the content file, while Dwork embeds the personal data in a decryption key), it would have been obvious to one of ordinary skill in the art to try the alternate location for embedding the personal data because it would have yielded the predictable result of providing the same function through a different implementation.

Although Dwork and Fujiwara disclose a string embedded in a digital file (Fujiwara, page 4, paragraph 0047; page 5, paragraphs 0049 and 0054), neither Wiser nor Fujiwara explicitly discloses embedding the string multiple times nor in a hidden manner. Stefik discloses a method for controlling use of digital works in which multiple watermarks may be embedded within a digital work, and both visible and invisible (i.e. hidden) watermarks may be used (column 8, lines 51-55). Stefik further discloses that the provider conveys a key to the public and that the file can be processed using the key to reveal the string in clear form (column 16, line 51-column 18, line 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the content of Dwork and Fujiwara to include the string embedded two or more times, at least once in a hidden manner, in order to increase robustness; that is, even if the visible string(s) is/are somehow removed, the invisible one(s) would remain and still allow control of the digital rights (see Stefik, column 8, lines 55-56).

In reference to Claim 58, Dwork, Fujiwara, and Stefik further disclose that a process to recover the string in clear form is conveyed to the public (Stefik, column 16, line 51-column 18, line 5).

### ***Conclusion***

16. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571)272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ZAD/

Examiner, Art Unit 2137

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2137